PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-098461
(43)Date of publication of application : 09.04.1999

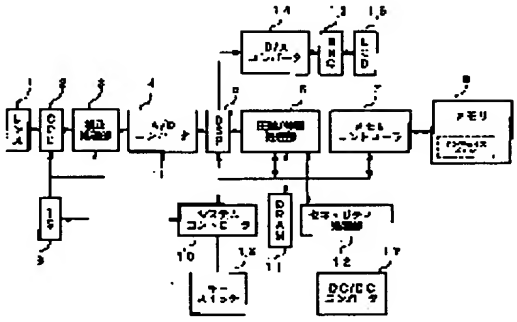
(51)Int.Cl. H04N 5/92
G06F 12/14
G09C 5/00
H04N 1/40
H04N 1/44
H04N 5/91

(21)Application number : 09-251185
(22)Date of filing : 16.09.1997

(71)Applicant : SHINKO ELECTRIC CO LTD
(72)Inventor : SUGIYAMA HAYAMI

(54) DIGITAL IMAGE RECORDER

(57)Abstract:
PROBLEM TO BE SOLVED: To check a forged image by using an inverse function of a unidirectional function employing a decoding key so as to encrypt index image data generated resulting from sampling received image data.
SOLUTION: Input data are given to a DSP 5, where the signal are converted into R, G, jB data corresponding to each pixel and the converted data are given to a compression/expansion processing section 6, in which the data are compressed and the compressed data are interleaved to produce index image data. Then a security processing section 12 applies an inverse function to a unidirectional function to the index image data to encrypt the data by means of decoding key data resulting in producing the encrypted index data. The encrypted index data with security are decoded as encrypted index data by using a unidirectional function and a public key data given in advance. Then the presence of forgery is discriminated by comparing the decoded data with original index image data.



LEGAL STATUS

[Date of request for examination] 22.01.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平11－98461
(43)公開日　平成11年(1999)４月９日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｎ	5/92		Ｈ０４Ｎ	5/92	Ｈ
Ｇ０６Ｆ	12/14	３１０	Ｇ０６Ｆ	12/14	３１０Ｚ
Ｇ０９Ｃ	5/00		Ｇ０９Ｃ	5/00	
Ｈ０４Ｎ	1/40		Ｈ０４Ｎ	1/44	
	1/44			1/40	Ｚ

審査請求　未請求　請求項の数９　ＯＬ　（全７頁）　最終頁に続く

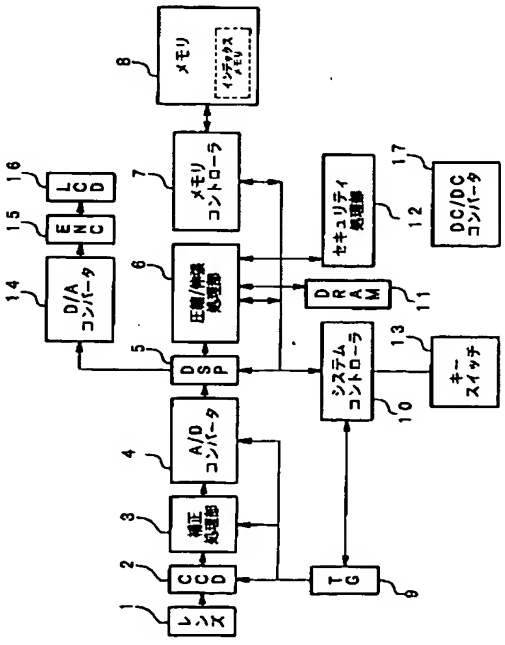
(21)出願番号　特願平9－251185

(22)出願日　平成９年(1997)９月16日

(71)出願人　000002059
神鋼電機株式会社
東京都江東区東陽七丁目２番14号
(72)発明者　杉山　早実
三重県伊勢市竹ヶ鼻町100番地　神鋼電機株式会社伊勢事業所内
(74)代理人　弁理士　志賀　正武　(外11名)

(54)【発明の名称】　デジタル画像記録装置

(57)【要約】
【課題】　改ざんが行われたインデックス画像のチェックができるデジタル画像記録装置と、さらに画像そのものにセキュリティをかけ改ざん不能にすることができるデジタル画像記録装置の提供。
【解決手段】　画像データ２１をサンプリングしたインデックス画像データに対して電子印鑑と同様の原理により、一方向関数の逆関数を使って復号鍵データによりセキュリティをかけ、画像データを暗号化し、このセキュリティをかけられた画像データは、一方向関数を使って、予め与えられている公開鍵２５データを用いることにより暗号化インデックスデータ２４を復元し、原インデックスデータとの比較により改ざんの有無をチェックすることができる。さらに、画像データそのものに同様のセキュリティをかけ暗号化圧縮画像データとし、改ざん不能にする。



【特許請求の範囲】

【請求項１】　デジタル画像記録装置が取り込んだ画像データをデータ処理して記憶する記憶手段と、該記憶手段の記憶データを記録する記録媒体と、該記録媒体からデータを読み出し、このデータの編集を行うためのパソコンと、前記編集後の画像データを印刷するプリンタまたは前記画像データをデジタルデータとして記録、保存する保存媒体とからなる画像処理システムにおいて、
前記デジタル画像記録装置が取り込んだ画像データをサンプリングしてインデックス画像データを作成し、該インデックス画像データに対し電子印鑑と同様の原理により復号鍵による一方向関数の逆関数を用いて暗号化することを特徴とするデジタル画像記録装置。

【請求項２】　前記記録、保存されるデータは下記５種類のデータがセットデータとして記録、保存されることを特徴とする請求項１に記載のデジタル画像記録装置。
（１）圧縮された画像データ
（２）画像に対応した個別情報データ
（３）復号鍵によって暗号化されたインデックス画像データ
（４）暗号化されたインデックス画像データを復元するための公開鍵
（５）圧縮画像データからインデックス画像データを作成する作成方法

【請求項３】　前記画像データ改ざんの有無を判定するために、
前記公開鍵による一方向関数を使って前記暗号化されたインデックス画像を復元することを特徴とする請求項１または２に記載のデジタル画像記録装置。

【請求項４】　前記画像データ改ざんの有無の判定するために、
前記画像データからインデックス画像を作成し、この画像と前記公開鍵による一方向関数を使ってインデックス画像データを復元することを特徴とする請求項１または２に記載のデジタル画像記録装置。

【請求項５】　デジタル画像記録装置が取り込んだ画像データをデータ処理して記憶する記憶手段と、該記憶手段の記憶データを記録する記録媒体と、該記録媒体からデータを読み出し、このデータの編集を行うためのパソコンと、前記編集後の画像データを印刷するプリンタまたは前記画像データをデジタルデータとして記録、保存する保存媒体とからなる画像処理システムにおいて、
前記デジタル画像記録装置が取り込んだ画像データに対し、電子印鑑と同様の原理により復号鍵による一方向関数の逆関数を用いて暗号化することを特徴とするデジタル画像記録装置。

【請求項６】　前記記録、保存されるデータは下記３種類のデータがセットデータとして記録、保存されることを特徴とする請求項５に記載のデジタル画像記録装置。
（１）暗号化された圧縮画像データ
（２）画像に対応した個別情報データ
（３）暗号化された圧縮画像データを復元するための公開鍵

【請求項７】　前記復号鍵のデータは読み出し不可能な不揮発メモリ等に記録されることを特徴とする請求項１ないし６のいずれかに記載のデジタル画像記録装置。

【請求項８】　前記復号鍵のデータは個々のデジタル画像記録装置に固有のデータであることを特徴とする請求項７に記載のデジタル画像記録装置。

【請求項９】　前記復号鍵のデータは複数台のデジタル画像記録装置に共通のデータであることを特徴とする請求項７に記載のデジタル画像記録装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、デジタル画像記録装置の画像処理のうち、特に画像セキュリティシステムに関する。

【０００２】

【従来の技術】従来、工事写真等、証拠を証明する目的で使用される写真は、専ら銀塩写真が用いられてきた。しかし、ＣＣＤイメージセンサを用いたデジタルカメラの普及につれて、業務効率改善の一環としてこのデジタルカメラが採用されるようになりつつある。

【０００３】デジタルカメラを使った写真システムを図３に示す。この写真システムの概略は、まず、デジタルカメラ３１で目的の写真を撮影すると、この画像は、ＣＣＤイメージセンサに取り込まれ、相関二重サンプリング、ガンマ補正、自動ホワイトバランスの各補正処理が行われた後、このアナログ信号はデジタル値に変換処理される。さらに、デジタル信号プロセッサ（ＤＳＰ）によって各ピクセルに対応したＲ，Ｇ，Ｂデータに変換され、画像データの圧縮が行われた後、メモリに保存される。このメモリには画像データの他、撮影条件、日付、画像ファイル記号などの付随情報が記録される。

【０００４】次に、パソコン３７に画像を転送する方法には二通りの手段があり、その第１は、メモリカード３４など何らかのメモリにデータを保存し、パソコン３７に読み込む方法であり、第２の方法は、デジタルカメラ３１本体のインターフェース３３とパソコン３７のインターフェース３６とを接続し、データを伝送する方法である。さらに、パソコン３７にインストールされているアルバム編集用ソフト４１によって、工事アルバムに編集する。編集結果はプリンタ３９によりプリント出力し、アルバムとしてバインドされる。また、この編集結果はＣＤＲ４０によってＣＤ－ＲＯＭに仕上げられ、デジタルデータとして記録、保存される。

【０００５】

【発明が解決しようとする課題】ところが上述の方法ではデータ転送、画像編集の段階で画像を改ざんしようと思えば、容易に改ざんすることができ、証拠写真として

の信頼性に欠けるという問題点の解決が課題となっていた。本発明はこのような背景の下になされたもので、改ざんが行われた画像のチェックができるデジタル画像記録装置の画像セキュリティシステムと、さらに画像そのものにセキュリティをかけ改ざん不能にすることができるデジタル画像記録装置の画像セキュリティシステムとを提供することを目的とする。

【０００６】

【課題を解決するための手段】請求項１に記載の発明は、デジタル画像記録装置が取り込んだ画像データをデータ処理して記憶する記憶手段と、該記憶手段の記憶データを記録する記録媒体と、該記録媒体からデータを読み出し、このデータの編集を行うためのパソコンと、前記編集後の画像データを印刷するプリンタまたは前記画像データをデジタルデータとして記録、保存する保存媒体とからなる画像処理システムにおいて、前記デジタル画像記録装置が取り込んだ画像データをサンプリングしてインデックス画像データを作成し、該インデックス画像データに対し電子印鑑と同様の原理により復号鍵による一方向関数の逆関数を用いて暗号化することを特徴とするデジタル画像記録装置を提供する。

【０００７】請求項２に記載の発明は、前記記録、保存されるデータが下記５種類のデータがセットデータとして記録、保存されることを特徴とする請求項１に記載のデジタル画像記録装置を提供する。

（１）圧縮された画像データ

（２）画像に対応した個別情報データ

（３）復号鍵によって暗号化されたインデックス画像データ

（４）暗号化されたインデックス画像データを復元するための公開鍵

（５）圧縮画像データからインデックス画像データを作成する作成方法

【０００８】請求項３に記載の発明は、前記画像データ改ざんの有無を判定するために、前記公開鍵による一方向関数を使って前記暗号化されたインデックス画像を復元することを特徴とする請求項１または２に記載のデジタル画像記録装置を提供する。

【０００９】請求項４に記載の発明は、前記画像データ改ざんの有無の判定するために、前記画像データからインデックス画像を作成し、この画像と前記公開鍵による一方向関数を使ってインデックス画像データを復元することを特徴とする請求項１または２に記載のデジタル画像記録装置を提供する。

【００１０】請求項５に記載の発明は、デジタル画像記録装置が取り込んだ画像データをデータ処理して記憶する記憶手段と、該記憶手段の記憶データを記録する記録媒体と、該記録媒体からデータを読み出し、このデータの編集を行うためのパソコンと、前記編集後の画像データを印刷するプリンタまたは前記画像データをデジタルデータとして記録、保存する保存媒体とからなる画像処理システムにおいて、前記デジタル画像記録装置が取り込んだ画像データに対し、電子印鑑と同様の原理により復号鍵による一方向関数の逆関数を用いて暗号化することを特徴とするデジタル画像記録装置を提供する。

【００１１】請求項６に記載の発明は、前記記録、保存されるデータが下記３種類のデータがセットデータとして記録、保存されることを特徴とする請求項５に記載のデジタル画像記録装置を提供する。

（１）暗号化された圧縮画像データ

（２）画像に対応した個別情報データ

（３）暗号化された圧縮画像データを復元するための公開鍵

【００１２】請求項７に記載の発明は、前記復号鍵のデータが読み出し不可能な不揮発メモリ等に記録されることを特徴とする請求項１ないし６のいずれかに記載のデジタル画像記録装置を提供する。

【００１３】請求項８に記載の発明は、前記復号鍵のデータが個々のデジタル画像記録装置に固有のデータであることを特徴とする請求項７に記載のデジタル画像記録装置を提供する。

【００１４】請求項９に記載の発明は、前記復号鍵のデータが複数台のデジタル画像記録装置に共通のデータであることを特徴とする請求項７に記載のデジタル画像記録装置を提供する。

【００１５】

【発明の実施の形態】以下、この発明の一実施形態について図を参照しながら説明する。なお、デジタルカメラを使った写真システムの構成は「従来の技術」の項で説明した図３と同一である。図１はこの発明の一実施形態による画像セキュリティシステムを備えたデジタルカメラの構成を示すブロック図であり、図２は画像セキュリティシステムによる電子ファイル構造のイメージ図である。

【００１６】図１において、符号１はデジタルカメラ３１のレンズ、符号２はＣＣＤイメージセンサ、符号３は相関二重サンプリング（ＣＤＳ）、ガンマ補正（γ）、自動ホワイトバランス（ＡＷＢ）処理を行う補正処理部、符号４はアナログ信号をデジタル値に変換するＡ／Ｄコンバータ、符号５はデータを各ピクセルに対応したＲ，Ｇ，Ｂデータに変換するデジタル信号プロセッサ（ＤＳＰ）である。

【００１７】符号６は画像データの圧縮／伸張処理部であり、メモリ８に格納する場合は例えば、ＪＰＥＧ方式などによりデータの圧縮を行い、メモリ８からデータを読み出しＬＣＤモニタ１６に表示する場合はデータの伸張を行う。符号７はメモリコントローラであり、画像データのメモリへの書き込みまたは読み出しを行う。符号８は画像データ以外に、この画像データとセットになる撮影条件、日付、画像ファイル記号などの付随情報が記

録されるメモリである。符号９はＣＣＤセンサからデータを取り出すためのタイミングパルス生成部（ＴＧ）、符号１０はデジタルカメラ３１のシステム全体の制御を行うシステムコントローラ、符号１１はＤＲＡＭであり、画像データ処理を行うとき、このデータを一時的に保存するためのメモリである。

【００１８】符号１２はセキュリティ処理部であり、前記圧縮／伸張処理部６と連携してデータの改ざん防止処理を行う。符号１３はキースイッチであり、デジタルカメラ３１を立ちあげるための電源スイッチである。符号１４はＤ／Ａコンバータであり、画像データに基づきＬＣＤをアクティブ化する。符号１５は写真画像を表示する液晶表示器（ＬＣＤ）１６の表示器コントローラ（ＥＮＣ）である。

【００１９】次に、図１および図３によるデジタルカメラを使った写真システムのシステム図を参照して、この発明の一実施形態の動作を説明する。デジタルカメラ３１で目的の写真を撮影し、このデジタルカメラ３１のレンズ１を通して撮影された画像は、ＣＣＤイメージセンサ２に取り込まれ、補正処理部３において相関二重サンプリング、ガンマ補正、自動ホワイトバランスの各補正処理が行われた後、Ａ／Ｄコンバータ４においてデジタル値に変換され、さらに、デジタル信号プロセッサ（ＤＳＰ）５によって各ピクセルに対応したＲ，Ｇ，Ｂデータに変換される。

【００２０】工事写真では撮影されたデータが撮影後に改ざんされては証拠写真としての信頼性に欠けるので改ざん防止の対策を講じるが、この改ざん防止の方式には２種類の方式がある。まず第１の方式は画像データが改ざんされた場合、改ざんされたことをチェックできる方式であり、この方式について以下に説明する。上述のＤＳＰ５によって各ピクセルに対応したＲ，Ｇ，Ｂデータに変換された信号は、圧縮／伸張処理部６において圧縮されたデータをさらに間引き、インデックス画像データを作成する。この場合単純な間引きより、原画像を大きな圧縮率で圧縮し、インデックス画像とする方が望ましい。

【００２１】また、保存画像とこれに対応するインデックスとには１対１に対応するファイル記号がつけられ、常に一体のものとして扱われる。つまり、圧縮／伸張処理部６は画像データの圧縮、伸張の他、インデックス作成機能も合わせ持つ。メモリコントローラ７は、圧縮した画像およびインデックス画像データのメモリ８への書き込みと、このメモリ８からのデータの読み出しをコントロールする。

【００２２】セキュリティ処理部１２は前記インデックス画像に対して、電子印鑑と同様の原理により、一方向関数の逆関数を使って復号２５鍵データによりセキュリティをかけて画像データを暗号化し、暗号化インデックスデータとする。このセキュリティをかけられた暗号化インデックスデータは、一方向関数を使って、予め与えられている公開鍵データを用いることにより暗号化インデックスデータとして復元することができ、原インデックス画像データとの比較により、データ改ざんの有無を判定することができる。

【００２３】上述の画像セキュリティシステムを備えたデジタルカメラから出力されるデータは次の５種類となり、図２（ａ）に示すように、電子記録メディアの電子ファイル２０に、リレーショナルな画像データセット２１として、次のようにセットで記録される。

（１）圧縮画像データ２２

（２）画像に対応した個別情報データ２３

（３）復号化キーでセキュリティのかけられた暗号化インデックスデータ２４

（４）セキュリティのかけられたインデックス画像データを復元するための公開鍵２５

（５）圧縮画像データからインデックスデータを作成するインデックス画像作成方法２６

【００２４】また、前記セキュリティ処理部１２の設定キーの中身は、数値あるいは計算式などのソフト的内容である。この設定キーが書き込まれるのは専用ＩＣであり、書き込みデータの設定はハード的に固定され、外部からこの書き込みデータを知ることは不可能である。もし、無理に調べようとすれば、ＩＣそのものが破損し、使用不可能になるようにすることもできる。また、セキュリティの設定は、基本的には個々のカメラに固有の値を設定するが、固有の値でなく共通の値とすることもできる。

【００２５】また、図２の画像ファイル２０に書き込まれる情報のうち、公開鍵２５、インデックス画像作成方法２６は必ずしも画像電子ファイル２０中に同時に書き込まれる必要はなく、例えばファイルの名称を一括に書き込んだインデックスファイル中に書き込むといった別の手段によって書き込んでも良い。

【００２６】これまでに説明してきたように、デジタルカメラからは画像データとセキュリティのかけられたインデックス画像が出力され、画像データはパソコンに取り込み画像の編集や画像の改ざんなどが自由に行えるが、セキュリティのかけられたインデックス画像は改ざんによりデータが破壊されてしまうので、改ざんは事実上不可能である。従って、写真画像が改ざんされたかどうかは、提出された写真画像と公開鍵を用いて復元したインデックス画像とを目視比較することによって改ざんされているかどうかをチェックすることができる。

【００２７】また、人間の目に頼らなくても画像データから、インデックスを作成したときと同一の処理を行ってインデックス画像データを作成し、この作成したインデックス画像データと公開鍵を用いて復元したインデックス画像データとが一致するかどうかをパソコンなどを使って検証することが可能となる。

【００２８】次に、データ改ざん防止の第２の方式について、上述の第１の方式と異なる部分について説明する。図１において、圧縮／伸張処理部６においてインデックスを作成せず、圧縮により作成された画像データそのものに復号鍵によって、セキュリティをかけ、メモリ７に格納する方式である。

【００２９】この方式では、上述の画像セキュリティシステムを備えたデジタルカメラから出力されるデータは次の３種類となり、図２（ｂ）に示すように、電子記録メディアの電子ファイル２０に、リレーショナルな画像データセット２１として、次のようにセットで記録される。

（１）暗号化して圧縮された暗号化圧縮画像データ２７
（２）画像に対応した個別情報データ２３
（３）セキュリティのかけられた暗号化圧縮画像データを復元するための公開鍵２５

この方式は、画像データそのものを暗号化するため信頼度が高いが、上述の第１の方式に比べ、暗号化と復号化に要する演算処理時間が長くなる。

【００３０】以上、本発明の一実施形態の動作を図面を参照して詳述してきたが、本発明はこの実施形態に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等があっても本発明に含まれる。例えば、工事写真に限定せず、スキャナ、ビデオなどデジタル画像を扱い、かつセキュリティが問題となる全てのケースに適用できる。

【００３１】

【発明の効果】これまでに説明したように、この発明の一実施形態の第１の方式によれば、画像データをサンプリングしたインデックス画像データに対して電子印鑑と同様の原理により、一方向関数の逆関数を使って復号鍵データによりセキュリティをかけ、画像データを暗号化し、このセキュリティをかけられた画像データは、一方向関数を使って、予め与えられている公開鍵データを用いることにより暗号化インデックスデータを復元するようにしたので、改ざんが行われた画像のチェックを行うことができるという効果が得られる。

【００３２】さらに、この発明の一実施形態の第２の方式によれば、画像データそのものにセキュリティをかけ改ざん不能にすることができるという効果が得られる。

【図面の簡単な説明】

【図１】　この発明の一実施形態による画像セキュリティシステムを備えたデジタルカメラの構成を示すブロック図である。

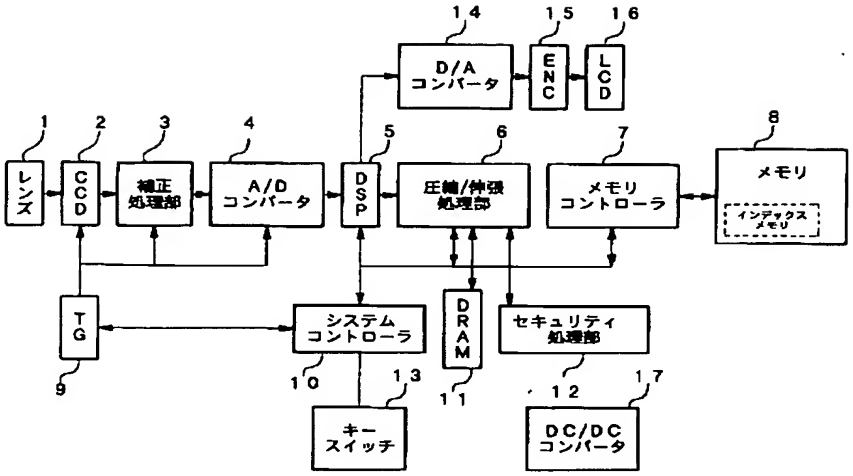
【図２】　画像セキュリティシステムによる電子ファイル構造のイメージ図である。

【図３】　デジタルカメラを使った写真システムを示す図である。

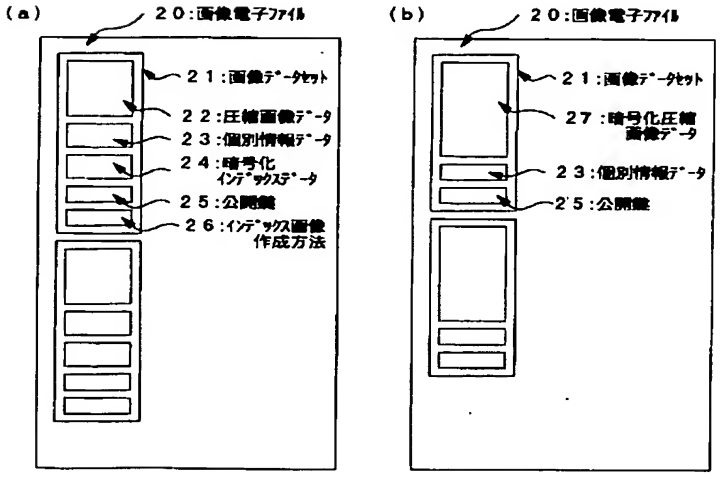
【符号の説明】

１　レンズ
２　ＣＣＤイメージセンサ（ＣＣＤ）
３　補正処理部
４　Ａ／Ｄコンバータ
５　デジタル信号プロセッサ（ＤＳＰ）
６　圧縮／伸張処理部
７　メモリコントローラ
８　メモリ
９　タイミングパルス生成部（ＴＧ）
１０　システムコントローラ
１１　ＤＲＡＭ
１２　セキュリティ処理部
１３　キースイッチ
１４　Ｄ／Ａコンバータ
１５　表示器コントローラ（ＥＮＣ）
１６　液晶表示器（ＬＣＤ）
１７　ＤＣ／ＤＣコンバータ
２０　画像電子ファイル
２１　画像データセット
２２　圧縮画像データ
２３　個別情報データ
２４　暗号化インデックスデータ
２５　公開鍵
２６　インデックス画像作成方法
２７　暗号化圧縮画像データ
３１　デジタルカメラ
３２　メモリカード挿入口
３３　インターフェース
３４　メモリカード
３５　ＰＣカードリーダ
３６　インターフェース
３７　パソコン
３８　ディスプレイ
３９　カラープリンタ
４０　ＣＤＲ
４１　アルバム編集ソフト

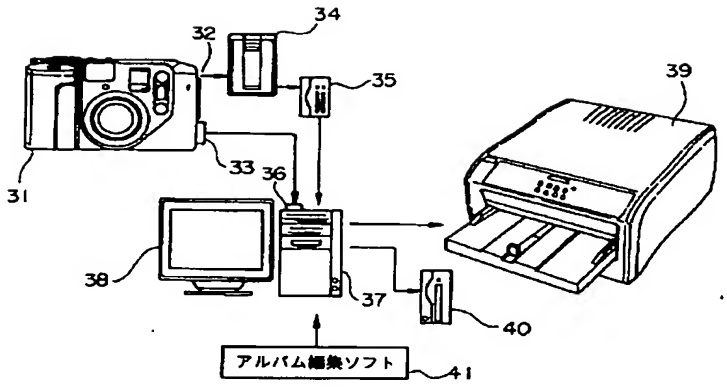
【図１】


14
15
16
D/A コンバータ
ENC
LCD
1
2
3
4
5
6
7
8
レンズ
CCD
補正処理部
A/D コンバータ
DSP
圧縮/伸張処理部
メモリコントローラ
メモリ
インデックスメモリ
TG
9
システムコントローラ
10
DRAM
11
セキュリティ処理部
12
13
キースイッチ
17
DC/DC コンバータ

【図２】


(a)
20:画像電子ファイル
21:画像データセット
22:圧縮画像データ
23:個別情報データ
24:暗号化インデックスデータ
25:公開鍵
26:インデックス画像作成方法
(b)
20:画像電子ファイル
21:画像データセット
27:暗号化圧縮画像データ
23:個別情報データ
25:公開鍵

【図３】



フロントページの続き

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｎ　5/91		Ｈ０４Ｎ　5/91	Ｎ